U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

July 25, 2013

Honorable Lewis A. Kaplan
United States District Judge
Southern District of New York
500 Pearl Street, Room 2240
New York, New York 10007

Re: *United States* v. *Valeri Aleksejev*, S2 11 Cr. 878 (LAK)

Dear Judge Kaplan:

Sentencing in the above-referenced matter is scheduled for July 30, 2013, at 2:30 p.m. The Government respectfully submits this memorandum in advance of sentencing to provide the Court with additional information regarding the relative roles of the defendants and the impact of the offenses of conviction. Details regarding the fraudulent scheme are in the Indictment and the Presentence Investigation Report ("PSR"), and will not be repeated here.

I. The Defendants' Roles

A. Vladimir Tsastsin

Tsastsin was the founder and leader of a company called Rove Digital since approximately early 2002. Since at least 2007, Tsastsin began using Rove Digital to commit online advertising fraud. Tsastsin had connections to coconspirators in Russia who provided him with the DNS Changer Malware. He also had Russian connections, including Andrey Taame, who had experience in selling fraudulent Internet traffic to online advertising networks. In approximately 2009, following negative publicity resulting from his conviction of Estonian felony charges (further discussed below), Tsastsin ceased using Rove Digital but continued its advertising fraud scheme by breaking up its functions among a number of different companies, nominally headed by certain of his co-defendants. For example, an entity named Infradata, which listed co-defendant Timur Gerassimenko as its sole board member, took over the computer programming side of the fraud scheme. Another company, named Novatech, which listed co-defendant Dmitri Jegorov as its sole board member, maintained the computer infrastructure/networking system which supported the fraud scheme. Tsastsin used still other companies – including the SPB Group, Cernel, Internet Path and others – to register domain names and IP addresses and to rent computer infrastructure that were used as instrumentalities of the fraud scheme. Tsastsin himself was the director of an entity named IT Consulting, but in fact was the leader and mastermind of the overall operation. (The various companies controlled by Tsastsin will be referred to, collectively, as the "Rove Companies.") In addition, Tsastsin also

operated a Danish entity named Furox APS, while his Russian partner and co-defendant Andrei Taame, operated companies named Lintor Ltd and Onwa Ltd, through which they sold hijacked (redirected) clicks to online advertisers. Payment records from advertising networks and bank records showed that U.S.-based advertisers alone paid out an aggregate of over $14 million to members of the conspiracy for the fraudulent web traffic. Bank records further showed that European advertisers paid millions more. The bulk of the money went into bank accounts controlled by Tsastsin, his wife, his parents, Taame, and Gerassimenko.

In addition to the fraud schemes described in the Indictment, Tsastsin and certain of his coconspirators also sold fake antivirus software to victims whose computers had been infected with scareware.

Other than the Rove Companies, Tsastsin also owned a domain registration company called EstDomains. EstDomains was notorious among network security / antivirus companies for registering websites for other cyber criminals engaged in various illegal schemes.[1]

Tsastsin also has a prior criminal history. He was convicted in Estonia in February 2008 of credit card fraud, money laundering, and document forgery.[2] As a result of Tsastsin's conviction, in late 2008, the Internet Corporation for Assigned Names and Numbers ("ICANN") – one of the main bodies responsible for governing the Internet and managing the routing of Internet addresses – revoked EstDomains' accreditation as a registrar, meaning that any IP address or domain name registered through EstDomains, for all practical purposes, would not exist on the Internet.

B. Timur Gerassimenko

Gerassimenko was Tsastsin's business partner and former classmate. As discussed above, he was the director of Infradata, which employed the code writers / programmers involved in the conspiracy. Among the Estonian defendants, he was Tsastsin's closest associate, serving as Tsastsin's second-in-command. Gerassimenko is also a programmer.

C. Dmitri Jegorov

As discussed above, Jegorov was the director of Novatech, which employed the network administrators involved in the conspiracy. Jegorov was himself a programmer and Ivanov's immediate supervisor. Among other things, he devised ways to prevent DNS Changer-infected computers from obtaining antivirus software updates. He also installed or supervised the installation of programming code that was designed to steal search data from Google. The stolen data was then used to create fake Google pages containing links that, when visited by DNS

---

[1] *See* http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html; http://www.informationweek.com/services/data/icann-shutting-down-estdomains-nov-24/212002478; http://www.secureworks.com/resources/blog/research/general-20841/.

[2] See http://www.icann.org/correspondence/burnette-to-tsastsin-28oct08-en.pdf.

Changer-infected computers, resolved to websites that enabled members of the conspiracy to monetize the visits.

D. VALERI ALEKSEJEV

ALEKSEJEV was initially hired as a programmer for Rove Digital in 2007. At the time of his arrest in November 2011, he was senior programmer for Infradata and reported directly to Gerassimenko. His responsibilities included devising ways to block DNS Changer Malware-infected computers from accessing antivirus software or operating system security updates, so that such software would not detect and remove the Malware; testing the Malware against various antivirus or operating system security programs to determine if they were capable of detecting the Malware hidden inside other software; and other programming projects to which he was assigned, including, for example, writing a program to conduct autoclicks on various websites in order to generate advertising revenue for the conspiracy.

The following are some of the emails which show the extent of ALEKSEJEV's knowledge of and involvement in the overall fraud:

1. On March 20, 2008, ALEKSEJEV received an email from Jegorov containing twenty-three subdomains belonging to major antivirus or operating system companies that were used to distribute security software updates. This email was the latest in an email string. The first email in the string, from Tsastsin to Jegorov, read "We need all these subdomains to fall in the non-resolved category." This meant that ALEKSEJEV was asked to ensure that DNS Changer-infected computers would not be able to obtain

2. On July 7, 2008, ALEKSEJEV sent Gerassimenko and Tsastsin an email attaching a screenshot from the Firefox/Mozilla search engine. The screenshot showed that the website "pcprivacycleaner.com" (a website the defendants operated or used to distribute the Malware) had been blocked as an "attack site," described as a site that tries "to install programs that steal private information, use your computer to attack others, or damage your system." In the email, ALEKSEJEV told Gerassimenko and Tsastsin that the new Firefox search engine blocked websites with potentially unreliable programs with its default settings, and therefore it was necessary to test Rove Digital's codecs (software for viewing videos, used to hide the Malware). In response, Gerassimenko wrote, "It is necessary to find out the location where he [the Internet user] requests IE [Internet Explorer] phishing filter and Firefox, and block those f[]cking sites."

3. On August 11, 2008, ALEKSEJEV sent an email to Tsastsin that contained a hyperlink to an article on the website of a well-known antivirus company, Trend Micro, entitled "Rogue Domain Name System Servers Part 2."[3] The article described "a network of more than 600 (apparently) identical rogue DNS servers, which IP

[3] *See* http://blog.trendmicro.com/trendlabs-security-intelligence/rogue-domain-name-system-servers-part-2/.

addresses are hardcoded in DNS-changing malware" and the "remarkable advanced technical and social engineering tricks" that define the corresponding DNS-changing Trojans. The article provided examples of how certain domain names were resolved by the rogue DNS servers to different domains along with their IP addresses. In ALEKSEJEV's email, below the hyperlink to this article, he wrote, "There are our IPs," and indicated that he would transfer one of the exposed domains to a new server. He also noted that "[t]here is a lot of traffic there."

4. In an August 26, 2008 email, after learning that the Avast antivirus program had alerted to the DNS Changer Malware in a digital file controlled by Rove Digital, Tsastsin instructed ALEKSEJEV to determine how the antivirus program was able to detect the Malware and to "block the [Avast anti-virus] update domain and watch its anti-virus activities...." Following those instructions, ALEKSEJEV determined that to block the antivirus update domain, "it [was] necessary to block all 999 hosts (something like: download1.avast.com - download999.avast.com)."

5. In a June 2, 2009 email, Gerassimenko forwarded to ALEKSEJEV an email from Tsastsin, which read in part: "Look the Indians don't want to give us the feeds but say let us put together whatever you need over here. Can we somehow send a person over to have him do the autoclicks over there? Or will the domain get seriously burned [meaning identified as being used for illicit activity] and hit with abuse complaints?" Gerassimenko asked ALEKSEJEV to "do some research whether it's possible to create an autoclick here through JS [javascript] like you did it on skenzo [a domain parking company; domain parking is a method for monetizing Internet traffic].

In short, while ALEKSEJEV was not a leader of the conspiracy, or the author of the DNS Changer source code, his contribution to the success of the conspiracy was significant. Arguably, blocking Malware-infected computers from obtaining antivirus and operating system security updates was the most harmful aspect of the scheme because it left the infected computers vulnerable to other forms of malware.

E. Konstantin Poltev

Poltev joined Rove Digital in 2005. After Tsastsin sold Rove Digital, Poltev transferred to IT Consulting. Because of his English-language ability, he was responsible for, among other things, handling abuse complaints about domains and IP addresses controlled by Rove Digital and the Rove Companies, identifying advertising partners for Furox APS and responding to their complaints when they detected low-quality or fraudulent Internet traffic, and registering domains that were used in the fraud scheme.

F. Anton Ivanov

Ivanov joined Rove Digital in approximately late 2006 or early 2007 as a system administrator. His job was to set up and secure servers and install applications. While the other

Estonian defendants appeared to have personal relationships that pre-dated their involvement in the conspiracy, the Government believes that Ivanov was only an employee.

II. Sentencing Factors

A. Seriousness of the Offense

The offense was serious and extremely sophisticated. As discussed in the Indictment and the Presentence Report, the defendant knowingly participated in a scheme to infect millions of computers worldwide with malware that blocked the computers' ability to update their antivirus protections and that turned the computers into instrumentalities of online advertising fraud for the coconspirators' own enrichment. To carry out this scheme, the co-defendants operated a vast network of servers, including approximately 50 rogue DNS servers, each with about two hard drives, located in New York at the time of the arrests. The larger servers received as many as 3,000 DNS resolution requests per second, while the smaller servers received several hundred requests per second.

The offense affected victims at numerous levels. At the most basic level, the victims included owners of infected computers who were redirected to websites not of their choosing and who were unable to obtain antivirus software updates. These victims include individuals, corporations, nonprofit organizations, and governmental entities. Given the large number of infected computers and victims, it is exceedingly difficult to estimate the total loss to this class of victims. However, by way of example, NASA, which had identified 135 incidents of DNS Changer infection in its network, incurred approximately $65,755 in remediation costs. *See* Exhibit A [to be provided]. Dell SecureWorks, a network security company, estimated that its enterprise customers likely spent in excess of $4 million (including the costs of replacing infected computers and security staff time) to respond to the Malware. *See* Exhibit B, at 2. A university located in the mid-west identified 46 incidents of DNS Changer infection, primarily on personally owned computers that logged onto the university's network.[4] These figures represent the damage to only a small fraction of the total number of estimated victims.

Victims also included advertisers who lost visitors who were potential customers; website operators who lost advertising revenue as a result of Web traffic that should have gone to their sites being redirected elsewhere; and advertisers and website operators who paid for worthless Internet traffic in that the visitors landed on their website not due to any real interest, but because of click hijacking. Although by no means a perfect measure, one estimate of the loss to this second class of victims is the amount of fraudulent proceeds that the members of the conspiracy derived from the overall scheme. In this regard, $14 million is a very conservative estimate of the pecuniary gain derived from the fraud. This sum represents payments by advertising networks in the United States for a limited period of time, but not necessarily for the entire period of their relationship with the Rove Companies. It also does not include payments from foreign advertising networks.

[4] The university decided not to submit a letter to the Court, but provided the information to the Government.

Another class of victims consist of the search engines that suffered reputational harm. When Internet users clicked on search results and found themselves redirected to random sites, they blamed the search engine. As Google, Inc. explained:

> First and foremost, when infected users clicked on a link in their Google search results, they would sometimes be redirected to a website selected by the malware instead of the actual website displayed in the search results. In addition, some users would sign in to Google services, but then would immediately be signed out again due to the fact that users were being redirected through the defendants' proxies. . . .
>
> The impacted users were unaware that they were infected with malware and, from their perspective, Google was the cause of the issues they were experiencing.

See Exhibit C, at 1-2. As a result, some Google users switched to its competitors' search engines. According to Google, hundreds of thousands of users of its search engine had been compromised by the DNS Changer Malware. *See id.* at 2. Google was not alone. The investigation revealed that virtually all of the largest U.S.-based Internet service providers ("ISPs") had been adversely affected. The $14 million estimated loss amount does not include the reputational harm to these ISPs.

Yet another class of victims is the antivirus companies which expended substantial resources to research complaints from their customers and fix the reported problems. For example, Dell SecureWorks estimated that it expended approximately $34,280 in responding to DNS Changer infections on its enterprise customers' computers.

Finally, the Government spent approximately $100,000 in remediation expenses. At the time the defendants were arrested, the FBI seized and disabled the defendants' rogue DNS servers. As the Court is aware, in order to ensure that infected computers that were connecting to the rogue DNS servers for DNS resolution did not suddenly lose the ability to access the Internet, the Government obtained Court authorization to hire the not-for-profit organization Internet Services Consortium to replace the rogue DNS servers with legitimate DNS servers for a period of months, to give the victims a chance to change their DNS settings and attempt to remove the Malware. The aggregate cost of that remediation effort amounted to approximately $100,000.

B. Need for Specific and General Deterrence and Just Punishment

Although the need for specific deterrence may be relatively low in this case, there is tremendous need for general deterrence. The anonymity of the Internet, the difficulty of determining which "clicks" are fraudulent, the huge sums of money involved in online advertising, the ability to spread the network infrastructure used to perpetuate click fraud across multiple countries, and the ease of operating far from where most victims are located, all

combine to make online advertising fraud increasingly attractive to cyber criminals. A substantial sentence is necessary to deter others from engaging in this type of cybercrime.

C. Characteristics of the Defendant

As noted in the Presentence Report, ALEKSEJEV has a college degree in computer science and is fluent in Russian, Estonian and English. (PSR ¶¶ 79-80). He was therefore better positioned than most defendants who appear before this Court to secure legitimate employment, but chose instead to participate in a fraudulent enterprise.

Although the Government does not dispute that ALEKSEJEV was a salaried employee, and does not appear to have earned more than his salary from the fraudulent scheme, his participation should not be dismissed as merely taking orders from others. His involvement was knowing from close to the start, if not from the very beginning, of his employment by Tsastsin. ALEKSEJEV was working at Rove Digital when Tsastsin was convicted of Estonian credit card fraud, money laundering and document forgery offenses in February 2008. ALEKSEJEV continued working with Tsastsin after he read and circulated the article on rogue DNS servers to his coconspirators in August 2008. And he remained with Tsastsin when Tsastsin's company EstDomains, which was notorious among Internet security companies for registering websites for cyber criminals, lost its registrar accreditation with ICANN. Moreover, the Estonian defendants all worked in a four-story building that was the size of a large townhouse, with easy access to one another. This was not a huge corporation in which employees in one department could be entirely unaware of operations in another department. Thus, while ALEKSEJEV was a salaried employee, he was fully aware of the illicit nature of the work he was doing and the criminal history of the person at the head of the enterprise.

III. The Defense's Arguments Are Untenable

The defense argues that the Court should disregard the Guidelines calculation in the plea agreement because "[t]here is ample reason to question whether the loss figure truly reflects the intrinsic wrongfulness of the charged conduct . . . ." Def. Mem. at 14. As explained in Section II.A above, the loss amount used to calculate the applicable Guidelines range *underestimates* the true extent of the aggregate financial loss to the multiple impacted parties. Moreover, the defendant has already benefitted from a two-level reduction in the Guidelines range (based on a loss amount of more than $2.5 million but not more than $7 million rather than the undisputed $14 million charged in the Indictment), to reflect his shorter period of involvement in the conspiracy. And as discussed in Section II.B, the fact that cyber criminals can pretend or attempt to argue that there are no "real" victims (as ALEKSEJEV appears to argue: "the offense was not of the same order of magnitude as a brazen scheme in which retirees were bilked out of their life savings . . . ."),[5] because the victims are generally anonymous to the perpetrators, is an argument for, not against, imposing a substantial sentence if there is to be any meaningful deterrence against cybercrime.

[5] *See* Def. Mem. at 14.

ALEKSEJEV also objects to being held accountable for a loss amount "based on the fortuity of the number of clicks by end users." Def. Mem. at 14-15. This argument should be rejected in light of the fact that he knew from the article regarding rogue DNS servers – which he circulated in August 2008 to his coconspirators – that the scheme involved hundreds of rogue DNS servers. There was no reason for such a large number of DNS servers unless a huge number of DNS requests were being redirected. Thus, the number of clicks, far being fortuitous, was entirely foreseeable to the coconspirators, including ALEKSEJEV.

ALEKSEJEV also argues that the enhancements based on the number of victims and the use of sophisticated means are unfairly duplicative because any scheme that affects a large number of victims is inherently sophisticated. This contention is of no merit. If ever a case warranted these enhancements, this one would be it. The six-level enhancement for the number of victims, pursuant to U.S.S.G. § 2B1.1(b)((2)(C), applies to any scheme involving more than 250 victims. The offenses of conviction here adversely affected millions of victims in over 100 countries. Similarly, the applicability of the two-level enhancement for using sophisticated means and committing the scheme from outside the United States, pursuant to U.S.S.G. § 2B1.1(b)(1), cannot be disputed. The conspiracy employed network infrastructure in at least Estonia, several states in the United States, and the Netherlands; used companies registered in the U.S., Russia and the Ukraine to register domain names and IP addresses; and opened bank accounts in the names of companies incorporated in Denmark, the Seychelles and Great Britain and Estonia to receive the proceeds of fraud. In this regard, it is worth noting that the Government could have, but did not, include a two-level enhancement for use of a special skill, pursuant to U.S.S.G. § 3B1.3.

CONCLUSION

For the reasons discussed above, the Government respectfully submits that a sentence within the Guidelines range of 97 to 121 months would be reasonable.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: /Sarah Y. Lai/
Sarah Y. Lai / James L. Pastore
Assistant United States Attorneys
(212) 637-1944 / 2418

cc: William J. Stampur, Esq.
(By electronic mail)